Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE
Thursday, March 24, 2016

Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector

One Defendant Also Charged with Obtaining Unauthorized Access into Control Systems of a New York Dam

A grand jury in the Southern District of New York indicted seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam (ITSEC) and Mersad Company (MERSAD), that performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks.

Ahmad Fathi, 37; Hamid Firoozi, 34; Amin Shokohi, 25; Sadegh Ahmadzadegan, aka Nitrojen26, 23; Omid Ghaffarinia, aka PLuS, 25; Sina Keissar, 25; and Nader Saedi, aka Turk Server, 26, launched DDoS attacks against 46 victims, primarily in the U.S financial sector, between late 2011 and mid-2013. The attacks disabled victim bank websites, prevented customers from accessing their accounts online and collectively cost the victims tens of millions of dollars in remediation costs as they worked to neutralize and mitigate the attacks on their servers. In addition, Firoozi is charged with obtaining unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, located in Rye, New York, in August and September of 2013.

The indictment was announced today by Attorney General Loretta E. Lynch, Director James B. Comey of the FBI, Assistant Attorney General for National Security John P. Carlin and U.S. Attorney Preet Bharara of the Southern District of New York.

"In unsealing this indictment, the Department of Justice is sending a powerful message: that we will not allow any individual, group, or nation to sabotage American financial institutions or undermine the integrity of fair competition in the operation of the free market," said Attorney General Lynch. "Through the work of our National Security Division, the FBI, and U.S. Attorney's Offices around the country, we will continue to pursue national security cyber threats through the use of all available tools, including public criminal charges. And as today's unsealing makes clear, individuals who engage in computer hacking will be exposed for their criminal conduct and sought for apprehension and prosecution in an American court of law."

"The FBI will find those behind cyber intrusions and hold them accountable — wherever they are, and whoever they are," said Director Comey. "By calling out the individuals and nations who use cyber attacks to threaten American enterprise, as we have done in this indictment, we will change behavior."

"Like past nation state-sponsored hackers, these defendants and their backers believed that they could attack our critical infrastructure without consequence, from behind a veil of cyber anonymity," said Assistant Attorney General Carlin. "This indictment once again shows there is no such veil – we can and

will expose malicious cyber hackers engaging in unlawful acts that threaten our public safety and national security."

"The charges announced today respond directly to a cyber-assault on New York, its institutions and its infrastructure," said U.S. Attorney Bharara. "The alleged onslaught of cyber-attacks on 46 of our largest financial institutions, many headquartered in New York City, resulted in hundreds of thousands of customers being unable to access their accounts and tens of millions of dollars being spent by the companies trying to stay online through these attacks. The infiltration of the Bowman Avenue dam represents a frightening new frontier in cybercrime. These were no ordinary crimes, but calculated attacks by groups with ties to Iran's Islamic Revolutionary Guard and designed specifically to harm America and its people. We now live in a world where devastating attacks on our financial system, our infrastructure and our way of life can be launched from anywhere in the world, with a click of a mouse. Confronting these types of cyber-attacks cannot be the job of just law enforcement. The charges announced today should serve as a wake-up call for everyone responsible for the security of our financial markets and for guarding our infrastructure. Our future security depends on heeding this call."

According to the indictment unsealed today in federal court in New York City:

DDoS Attacks

The DDoS campaign began in approximately December 2011, and the attacks occurred only sporadically until September 2012, at which point they escalated in frequency to a near-weekly basis, between Tuesday and Thursdays during normal business hours in the United States. On certain days during the campaign, victim computer servers were hit with as much as 140 gigabits of data per second and hundreds of thousands of customers were cut off from online access to their bank accounts.

Fathi, Firoozi and Shokohi were responsible for ITSEC's portion of the DDoS campaign against the U.S. financial sector and are charged with one count of conspiracy to commit and aid and abet computer hacking. Fathi was the leader of ITSEC and was responsible for supervising and coordinating ITSEC's portion of the DDoS campaign, along with managing computer intrusion and cyberattack projects being conducted for the government of Iran. Firoozi was the network manager at ITSEC and, in that role, procured and managed computer servers that were used to coordinate and direct ITSEC's portion of the DDoS campaign. Shokohi is a computer hacker who helped build the botnet used by ITSEC to carry out its portion of the DDoS campaign and created malware used to direct the botnet to engage in those attacks. During the time that he worked in support of the DDoS campaign, Shokohi received credit for his computer intrusion work from the Iranian government towards his completion of his mandatory military service requirement in Iran.

Ahmadzadegan, Ghaffarinia, Keissar and Saedi were responsible for managing the botnet used in MERSAD's portion of the campaign, and are also charged with one count of conspiracy to commit and aid and abet computer hacking. Ahmadzadegan was a co-founder of MERSAD and was responsible for managing the botnet used in MERSAD's portion of the DDoS campaign. He was also associated with Iranian hacking groups Sun Army and the Ashiyane Digital Security Team (ADST), and claimed responsibility for hacking servers belonging to the National Aeronautics and Space Administration (NASA) in February 2012. Ahmadzadegan has also provided training to Iranian intelligence personnel. Ghaffarinia was a co-founder of MERSAD and created malicious computer code used to compromise computer servers and build MERSAD's botnet. Ghaffarinia was also associated with Sun Army and ADST, and has also claimed responsibility for hacking NASA servers in February 2012, as well

as thousands of other servers in the United States, the United Kingdom and Israel. Keissar procured computer servers used by MERSAD to access and manipulate MERSAD's botnet, and also performed preliminary testing of the same botnet prior to its use in MERSAD's portion of the DDoS campaign. Saedi was an employee of MERSAD and a former Sun Army computer hacker who expressly touted himself as an expert in DDoS attacks. Saedi wrote computer scripts used to locate vulnerable servers to build the MERSAD botnet used in its portion of the DDoS campaign.

For the purpose of carrying out the attacks, each group built and maintained their own botnets, which consisted of thousands of compromised computer systems owned by unwitting third parties that had been infected with the defendants' malware, and subject to their remote command and control. The defendants and/or their unindicted co-conspirators then sent orders to their botnets to direct significant amounts of malicious traffic at computer servers used to operate the websites for victim financial institutions, which overwhelmed victim servers and disabled them from customers seeking to legitimately access the websites or their online bank accounts. Although the DDoS campaign caused damage to the financial sector victims and interfered with their customers' ability to do online banking, the attacks did not affect or result in the theft of customer account data.

DDoS Botnet Remediation

Since the attacks, the Department of Justice and the FBI have worked together with the private sector to effectively neutralize and remediate the defendants' botnets. Specifically, through approximately 20 FBI Liaison Alert System (FLASH) messages, the FBI regularly provided updated information collected from the investigation regarding the identity of systems that been infected with the defendants' malware and operating as bots within the malicious botnets. In addition, the FBI conducted extensive direct outreach to Internet service providers responsible for hosting systems that have been infected with the defendants' malware to provide them information and assistance in removing the malware to protect their customers and other potential victims of the defendants' unlawful cyber activities. Through these outreach efforts and the cooperation of the private sector, over 95 percent of the known part of the defendants' botnets have been successfully remediated.

Bowman Dam Intrusion

Between Aug. 28, 2013, and Sept. 18, 2013, Firoozi repeatedly obtained unauthorized access to the SCADA systems of the Bowman Dam, and is charged with one substantive count of obtaining and aiding and abetting computer hacking. This unauthorized access allowed him to repeatedly obtain information regarding the status and operation of the dam, including information about the water levels, temperature and status of the sluice gate, which is responsible for controlling water levels and flow rates. Although that access would normally have permitted Firoozi to remotely operate and manipulate the Bowman Dam's sluice gate, Firoozi did not have that capability because the sluice gate had been manually disconnected for maintenance at the time of the intrusion.

Remediation for the Bowman Dam intrusion cost over $30,000.

* * *

All seven defendants face a maximum sentence of 10 years in prison for conspiracy to commit and aid and abet computer hacking. Firoozi faces an additional five years in prison for obtaining and aiding and abetting unauthorized access to a protected computer at the Bowman Dam.

An indictment is merely an accusation and all defendants are presumed innocent unless proven guilty in a court of law.

The case was investigated by the FBI, including the Chicago; Cincinnati; New York; Newark, New Jersey; Phoenix; and San Francisco Field Offices. This case is being prosecuted by Assistant U.S. Attorney Timothy T. Howard of the Southern District of New York, with the substantial assistance of Deputy Chief Sean M. Newell of the National Security Division's Counterintelligence and Export Control Section.

16-348

Topic:
National Security